

## EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	10	(plessier and bernard).in. and modular	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 10:42
L2	44	@ad<"20040331" and Montgomery and (modulo or mod or modular) and (carry-save or (carry adj save))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 10:52
L3	153	@ad<"20040331" and Montgomery and (modulo or mod or modular) and "708"/\$.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 10:52
L4	117	@ad<"20040331" and Montgomery and (modulo or mod or modular). clm. and "708"/\$.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 10:52
L5	26	3 and (carry-save or (carry adj save))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 10:53
L6	0	5 not 2	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 10:53
L7	416	708/491-492.ccls. and @ad<"20040331" and (modulo or mod or modular)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 10:55
L8	120	7 and Montgomery	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 10:54

## EAST Search History

L9	108	8 and (modulo or mod or modular). clm,ab,ti.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 10:55
L10	89	9 not 2	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 10:55
L11	49	10 and adder\$1	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 10:56
L12	6	("5745398"   "5764554"   "5948051"   "6035317").PN. OR ("6275837"). URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/07/25 11:00
L13	0	(10/789311).APP.	USPAT; USOCR	OR	ON	2007/07/25 11:01
L14	0	(10/800181).APP.	USPAT; USOCR	OR	ON	2007/07/25 11:01

Author Search[BROWSE](#)[SEARCH](#)[IEEE XPLORE GUIDE](#)[SUPPORT](#)**② OPTION 1****Quick Find an Author:**

Enter a name to locate articles written by that author.

**>>**

Select a name to view articles written by that author

[Plessier, B.](#)[Plessier, B.F.](#)

Example: Enter Lockett S to obtain a list of authors with the last name Lockett and the first initial S.

**③ OPTION 2****Browse alphabetically**

Select a letter from the list.

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)[Help](#) [Contact Us](#) [Privacy & Security](#) [IEEE.org](#)

© Copyright 2006 IEEE – All Rights Reserved

Indexed by  
 Inspec®

□ Search Results

BROWSE

SEARCH

IEEE Xplore Guide

SUPPORT

Results for "(plessier b.<in>au)"

Your search matched 10 of 1621473 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by **Relevance** in **Descending** order.

 e-mail  printer friendly

» Search Options

[View Session History](#)

[New Search](#)

Modify Search

(plessier b.<in>au)

[Search](#) 

Check to search only within this results set

Display Format:  Citation  Citation & Abstract

[view selected items](#) [Select All](#) [Deselect All](#)

» Key

IEEE JNL IEEE Journal or Magazine

IET JNL IET Journal or Magazine

IEEE CNF IEEE Conference Proceeding

IET CNF IET Conference Proceeding

IEEE STD IEEE Standard

1. **Algorithms for approximate FSM traversal based on state space decomposition**  
Hyunwoo Cho; Hachtel, G.D.; Macii, E.; Plessier, B.; Somenzi, F.;  
Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on  
Volume 15, Issue 12, Dec. 1996 Page(s):1465 - 1478  
Digital Object Identifier 10.1109/43.552080  
[AbstractPlus](#) | [References](#) | [Full Text: PDF\(480 KB\)](#) IEEE JNL  
[Rights and Permissions](#)

2. **Formal verification of digital systems by automatic reduction of data paths**  
Macii, E.; Plessier, B.; Somenzi, F.;  
Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on  
Volume 16, Issue 10, Oct. 1997 Page(s):1136 - 1156  
Digital Object Identifier 10.1109/43.662676  
[AbstractPlus](#) | [References](#) | [Full Text: PDF\(804 KB\)](#) IEEE JNL  
[Rights and Permissions](#)

3. **Algorithms for Approximate FSM Traversal**  
Hyunwoo Cho; Hachtel, G.D.; Macii, E.; Plessier, B.; Somenzi, F.;  
Design Automation, 1993. 30th Conference on  
14-18 June 1993 Page(s):25 - 30  
[AbstractPlus](#) | [Full Text: PDF\(728 KB\)](#) IEEE CNF  
[Rights and Permissions](#)

4. **Formal verification of a commercial serial bus interface**  
Plessier, B.; Pixley, C.;  
Computers and Communications, 1995. Conference Proceedings of the 1995 IEEE Fourteenth Annual International Phoenix Conference on  
28-31 March 1995 Page(s):378 - 382  
Digital Object Identifier 10.1109/PCCC.1995.472465  
[AbstractPlus](#) | [Full Text: PDF\(440 KB\)](#) IEEE CNF  
[Rights and Permissions](#)

5. **ATPG aspects of FSM verification**  
Cho, H.; Hachtel, G.; Jeong, S.-W.; Plessier, B.; Schwarz, E.; Somenzi, F.;  
Computer-Aided Design, 1990. ICCAD-90. Digest of Technical Papers., 1990 IEEE International Conference on  
11-15 Nov. 1990 Page(s):134 - 137  
Digital Object Identifier 10.1109/ICCAD.1990.129861  
[AbstractPlus](#) | [Full Text: PDF\(348 KB\)](#) IEEE CNF  
[Rights and Permissions](#)

6. **Variable ordering and selection of FSM traversal**  
Jeong, S.-W.; Plessier, B.; Hachtel, G.D.; Somenzi, F.;

7. **Extended BDD's: trading off canonicity for structure in verification algorithms**

Jeong, S.-W.; Plessier, B.; Hachtel, G.; Somenzi, F.;

[Computer-Aided Design, 1991. ICCAD-91. Digest of Technical Papers.. 1991 IEEE International Conference on](#)

11-14 Nov. 1991 Page(s):464 - 467

Digital Object Identifier 10.1109/ICCAD.1991.185305

[AbstractPlus](#) | Full Text: [PDF\(332 KB\)](#) IEEE CNF

[Rights and Permissions](#)

8. **Verification of systems containing counters**

Macii, E.; Plessier, B.; Somenzi, F.;

[Computer-Aided Design, 1992. ICCAD-92. Digest of Technical Papers.. 1992 IEEE/ACM International Conference on](#)

8-12 Nov. 1992 Page(s):179 - 182

Digital Object Identifier 10.1109/ICCAD.1992.279378

[AbstractPlus](#) | Full Text: [PDF\(368 KB\)](#) IEEE CNF

[Rights and Permissions](#)

9. **Variable ordering for binary decision diagrams**

Jeong, S.-W.; Plessier, B.; Hachtel, G.D.; Somenzi, F.;

[Design Automation, 1992. Proceedings. \[3rd\] European Conference on](#)

16-19 March 1992 Page(s):447 - 451

Digital Object Identifier 10.1109/EDAC.1992.205974

[AbstractPlus](#) | Full Text: [PDF\(448 KB\)](#) IEEE CNF

[Rights and Permissions](#)

10. **Symmetry Detection And Dynamic Variable**

Panda, S.; Somenzi, F.; Plessier, B.F.;

[Computer-Aided Design, 1994.. IEEE/ACM International Conference on](#)

November 6-10, 1994 Page(s):628 - 631

[AbstractPlus](#) | Full Text: [PDF\(480 KB\)](#) IEEE CNF

[Rights and Permissions](#)

## □ Search Results

BROWSE

SEARCH

IEEE Xplore Guide

SUPPORT

Results for "(plessier b.f.&lt;in&gt;au)"

Your search matched 1 of 1621473 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by **Relevance** in **Descending** order. e-mail  printer friendly

## » Search Options

[View Session History](#)[New Search](#)

## Modify Search

(plessier b.f.&lt;in&gt;au)

[Search](#) 

## » Key

IEEE JNL IEEE Journal or Magazine

IET JNL IET Journal or Magazine

IEEE CNF IEEE Conference Proceeding

IET CNF IET Conference Proceeding

IEEE STD IEEE Standard

 Check to search only within this results setDisplay Format:  Citation  Citation & Abstract[view selected items](#) [Select All](#) [Deselect All](#) 1. Symmetry Detection And Dynamic Variable

Panda, S.; Somenzi, F.; Plessier, B.F.;  
Computer-Aided Design, 1994., IEEE/ACM International Conference on  
November 6-10, 1994 Page(s):628 - 631

[AbstractPlus](#) | Full Text: [PDF\(480 KB\)](#) IEEE CNF  
[Rights and Permissions](#)

Help Contact Us Privacy &amp; Security IEEE.org

© Copyright 2006 IEEE – All Rights Reserved

[Search Results](#)[BROWSE](#)[SEARCH](#)[IEEE XPLORER GUIDE](#)[SUPPORT](#)

Results for "((montgomery <and> ((carry save) <or> (carry-save)) <and> (partial product))<in..."  
Your search matched 0 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by **Relevance** in **Descending** order.

 [e-mail](#) [printer friendly](#)[» Search Options](#)[View Session History](#)[New Search](#)[Modify Search](#) Check to search only within this results setDisplay Format:  Citation  Citation & Abstract[» Key](#)

IEEE JNL IEEE Journal or Magazine

IET JNL IET Journal or Magazine

IEEE CNF IEEE Conference Proceeding

IET CNF IET Conference Proceeding

IEEE STD IEEE Standard

**No results were found.**

Please edit your search criteria and try again. Refer to the Help pages if you need assistance revising your search.

[Help](#) [Contact Us](#) [Privacy & Security](#) [IEEE.org](#)

© Copyright 2006 IEEE – All Rights Reserved

[Search Session History](#)

[BROWSE](#)

[SEARCH](#)

[IEEE XPLOR GUIDE](#)

[SUPPORT](#)

Wed, 25 Jul 2007, 11:08:39 AM EST

Search Query Display

Edit an existing query or  
compose a new query in the  
Search Query Display.

Select a search number (#)  
to:

- Add a query to the Search Query Display
- Combine search queries using AND, OR, or NOT
- Delete a search
- Run a search

Recent Search Queries

		Results
<a href="#">#1</a>	(plessier b.<in>au)	10
<a href="#">#2</a>	(plessier b.<in>au)	10
<a href="#">#3</a>	(plessier b.f.<in>au)	1
<a href="#">#4</a>	((montgomery <and> ((carry save) <or> (carry-save)) <and> (partial product))<in>metadata)	0

[Help](#) [Contact Us](#) [Privacy & Security](#) [IEEE.org](#)

© Copyright 2006 IEEE – All Rights Reserved

Montgomery modular multiplier and method thereof using carry save ...

Montgomery modular multiplier and method thereof using carry save addition. Document

Type and Number: ... Images are available in PDF form when logged in. ...

[www.freepatentsonline.com/EP1471420.html](http://www.freepatentsonline.com/EP1471420.html) - 75k - [Cached](#) - [Similar pages](#)

Method and apparatus for performing montgomery multiplications ...

The Montgomery multiplication is a commonly used method for performing the ... Each basic operation may comprise an addition or a carry-save addition ...

[www.freepatentsonline.com/20060059220.html](http://www.freepatentsonline.com/20060059220.html) - 59k - Supplemental Result -

[Cached](#) - [Similar pages](#)

[ More results from [www.freepatentsonline.com](http://www.freepatentsonline.com) ]

[PDF] Carry-save montgomery modular exponentiation on reconfigurable ...

File Format: PDF/Adobe Acrobat

process, while the Montgomery's method does not. This is .... Algorithm 2 - Carry-Save

Montgomery Product MonProd(A,B). radix-2. Given N = ...

[ieeexplore.ieee.org/iel5/8959/28392/01269231.pdf?arnumber=1269231](http://ieeexplore.ieee.org/iel5/8959/28392/01269231.pdf?arnumber=1269231) - [Similar pages](#)

Carry-Save Montgomery Modular Exponentiation on Reconfigurable ...

Carry-Save Montgomery Modular Exponentiation on Reconfigurable Hardware (2004) ... 6

A Method for Obtaining Digital Signatures (context) - Rivest - 1978 ...

[citeseer.ist.psu.edu/cilardo04carrysave.html](http://citeseer.ist.psu.edu/cilardo04carrysave.html) - 19k - [Cached](#) - [Similar pages](#)

A Staged Carry-Save-Adder Array for Montgomery Modular ...

Abstract: In this paper, an efficient VLSI architecture to compute the n-bit Montgomery modular multiplication is proposed. By using the staged carry save ...

[citeseer.ist.psu.edu/661814.html](http://citeseer.ist.psu.edu/661814.html) - 19k - [Cached](#) - [Similar pages](#)

Apparatus & method for modular multiplication & exponentiation ...

the multiplicand values to be switched in turn into the carry save adder ..... Reference is also made to the Montgomery multiplication methods as MM. ...

[www.patentmonkey.com/PM/patentid/6185596.aspx](http://www.patentmonkey.com/PM/patentid/6185596.aspx) - 201k - Supplemental Result -

[Cached](#) - [Similar pages](#)

Apparatus and method for modular multiplication and exponentiation ...

Reference is also made to the Montgomery multiplication methods as MM. ..... B.sub.d ; ii the LS Carry Out bit from the Carry Save Accumulator; ...

[www.patentmonkey.com/PM/patentid/6748410.aspx](http://www.patentmonkey.com/PM/patentid/6748410.aspx) - 250k - Supplemental Result -

[Cached](#) - [Similar pages](#)

[PDF] An Efficient Hardware Architecture for Factoring Integers with the ...

File Format: PDF/Adobe Acrobat - [View as HTML](#)

While in [6] a structure with carry-save adders and redundant .... [9] P. Montgomery,

"Speeding up the Pollard and elliptic curve methods of factorization" ...

[cr.yp.to/bib/2005/franke-ecm.pdf](http://cr.yp.to/bib/2005/franke-ecm.pdf) - [Similar pages](#)

[PDF] A Complexity-Effective Version of Montgomery's Algorithm

File Format: PDF/Adobe Acrobat - [View as HTML](#)

The standard Montgomery method for modular multiplication is ... Carry save adders have a latency of O(1) in comparison to standard ripple ...

[www.ece.rochester.edu/~albonesi/wced02/papers/bunimov.pdf](http://www.ece.rochester.edu/~albonesi/wced02/papers/bunimov.pdf) - [Similar pages](#)

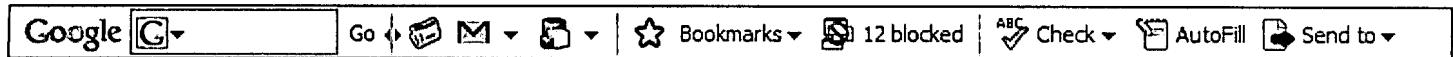
Apparatus & method for modular multiplication & exponentiation ...

Apparatus as in claim 1 wherein summations into the carry save adder are .... Reference is also made to the Montgomery multiplication methods as MM. ...

1 [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#)

[Next](#)

Free! Get the Google Toolbar. [Download Now](#) - [About Toolbar](#)



Montgomery method carry-save pdf | [Search](#)

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied? Help us improve](#)

©2007 Google - [Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

Google

Montgomery method carry-save pdf

Search

Advanced Search

Preferences

Web

Results 21 - 30 of about 704 for Montgomery method carry-save pdf. (0.16 seconds)[PDF] Fast Montgomery Modular Multiplication and RSA Cryptographic ...File Format: PDF/Adobe Acrobat - [View as HTML](#)Montgomery's multiplication algorithm are presented. These use. **Carry Save Adders** (CSAs) to perform the large word length ...[eee.ucc.ie/staff/marnanel/Files/papers/Mclvor\\_Asilomar2003.pdf](http://eee.ucc.ie/staff/marnanel/Files/papers/Mclvor_Asilomar2003.pdf) - [Similar pages](#)[PDF] A Scalable Dual Mode Arithmetic Unit for Public Key CryptosystemsFile Format: PDF/Adobe Acrobat - [View as HTML](#)tiplications and squarings using the R-L binary **method** [5]. ..... based **Montgomery** multiplier using **carry save** addition is. presented in [13]. ...[eee.ucc.ie/staff/marnanel/Files/papers/Fran-ITCC05.pdf](http://eee.ucc.ie/staff/marnanel/Files/papers/Fran-ITCC05.pdf) - [Similar pages](#)[PDF] A Unified, Reconfigurable Architecture for Montgomery ...

File Format: PDF/Adobe Acrobat

an algorithm to compute **Montgomery** multiplication. using **carry-save** arithmetic in GF(p).But the ..... R.L et al., "A **method** for obtaining Digital ...[doi.ieeecomputersociety.org/10.1109/VLSID.2007.27](http://doi.ieeecomputersociety.org/10.1109/VLSID.2007.27) - [Similar pages](#)[PDF] A Staged Carry-Save-Adder Array for Montgomery Modular MultiplicationFile Format: PDF/Adobe Acrobat - [View as HTML](#)Montgomery modular multiplication is proposed. By using the. staged **carry save** adder (CSA) array, the computation cycles of. addition reduced about 3n/8. ...[www.ap-asic.org/2002/2B-5.pdf](http://www.ap-asic.org/2002/2B-5.pdf) - [Similar pages](#)[PDF] 1 Introduction 2 Montgomery Multiplication AlgorithmFile Format: PDF/Adobe Acrobat - [View as HTML](#)Montgomery algorithm can be used3, 4, 5]. An attractive **method** for faster ... saved in **carry save** form representation and the input operands are assumed to ...[is.hoseo.ac.kr/paper/jwisc\\_form2.pdf](http://is.hoseo.ac.kr/paper/jwisc_form2.pdf) - [Supplemental Result](#) - [Similar pages](#)[PDF] Comparison of Two Implementations of Scalable Montgomery ...File Format: PDF/Adobe Acrobat - [View as HTML](#)able Montgomery Modular Multiplication (MM) coprocessor ..... as originally proposed PE based on **carry-save** adders. The. new **method** uses only 80% of the ...[www.best.tuke.sk/simka/download/pub/dru\\_fis\\_sim\\_04.pdf](http://www.best.tuke.sk/simka/download/pub/dru_fis_sim_04.pdf) - [Similar pages](#)[PDF] Efficient Architectures for implementing Montgomery Modular ...

File Format: PDF/Adobe Acrobat

Section 3 introduces the **Montgomery method** of modular. multiplication and presents 3 variations ..... uses a **Double Carry Save Adder** (CSA) structure with an ...[portal.acm.org/ft\\_gateway.cfm?id=503055&type=pdf](http://portal.acm.org/ft_gateway.cfm?id=503055&type=pdf) - [Similar pages](#)Memory request handling **method** for small discontiguous accesses to ...Method for the implementation of modular reduction according to the **Montgomery method**

Issued on: June 9, 1998 Inventor: Monier 5771369 Memory row redrive ...

[www.patentstorm.us/patents/6910095.html](http://www.patentstorm.us/patents/6910095.html) - 25k - [Cached](#) - [Similar pages](#)Apparatus and **method** for modular multiplication and exponentiation ...iii) then adding to this summation; as it serially exits the **Carry Save** k+1 Bit ..... UsingMontgomery's modular reduction **method**, division is typically ...[www.wkipatents.com/6748410.html](http://www.wkipatents.com/6748410.html) - 358k - [Cached](#) - [Similar pages](#)[PDF] Architectural Extensions for Elliptic Curve Cryptography over GF(2<sup>n</sup>)File Format: PDF/Adobe Acrobat - [View as HTML](#)Integer multipliers typically use a **carry-save** adder (CSA) tree together with ....<http://www.google.com/search?q=Montgomery+method+carry-save+pdf&hl=en&start=20&sa=N>

7/25/07

[Previous](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#) [Next](#)

---

Montgomery method carry-save pdf

[Search within results](#) | [Language Tools](#) | [Search Tips](#)

---

©2007 Google - [Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

[Google](#)

Montgomery method carry-save pdf

[Advanced Search](#)[Preferences](#)

Web

Results 1 - 10 of about 701 for Montgomery method carry-save pdf. (0.37 seconds)

### Montgomery modular multiplier and method thereof using carry save ...

Montgomery modular multiplier and method thereof using **carry save** addition. Document

Type and Number: ... Images are available in **PDF** form when logged in. ...

[www.freepatentsonline.com/EP1471420.html](http://www.freepatentsonline.com/EP1471420.html) - 75k - [Cached](#) - [Similar pages](#)

### Method and apparatus for performing montgomery multiplications ...

The **Montgomery** multiplication is a commonly used **method** for performing the ... Each basic operation may comprise an addition or a **carry-save** addition ...

[www.freepatentsonline.com/20060059220.html](http://www.freepatentsonline.com/20060059220.html) - 59k - Supplemental Result -

[Cached](#) - [Similar pages](#)

[ More results from [www.freepatentsonline.com](http://www.freepatentsonline.com) ]

### [PDF] Carry-save montgomery modular exponentiation on reconfigurable ...

File Format: PDF/Adobe Acrobat

process, while the **Montgomery's method** does not. This is .... Algorithm 2 - **Carry-Save Montgomery** Product MonProd(A,B). radix-2. Given N = ...

[ieeexplore.ieee.org/iel5/8959/28392/01269231.pdf?arnumber=1269231](http://ieeexplore.ieee.org/iel5/8959/28392/01269231.pdf?arnumber=1269231) - [Similar pages](#)

### Carry-Save Montgomery Modular Exponentiation on Reconfigurable ...

**Carry-Save Montgomery** Modular Exponentiation on Reconfigurable Hardware (2004) ... 6

A Method for Obtaining Digital Signatures (context) - Rivest - 1978 ...

[citeseer.ist.psu.edu/cilardo04carrysave.html](http://citeseer.ist.psu.edu/cilardo04carrysave.html) - 19k - [Cached](#) - [Similar pages](#)

### A Staged Carry-Save-Adder Array for Montgomery Modular ...

Abstract: In this paper, an efficient VLSI architecture to compute the n-bit **Montgomery** modular multiplication is proposed. By using the staged **carry save** ...

[citeseer.ist.psu.edu/661814.html](http://citeseer.ist.psu.edu/661814.html) - 19k - [Cached](#) - [Similar pages](#)

### Apparatus & method for modular multiplication & exponentiation ...

the multiplicand values to be switched in turn into the **carry save** adder ..... Reference is

also made to the **Montgomery** multiplication **methods** as MM. ...

[www.patentmonkey.com/PM/patentid/6185596.aspx](http://www.patentmonkey.com/PM/patentid/6185596.aspx) - 201k - Supplemental Result -

[Cached](#) - [Similar pages](#)

### Apparatus and method for modular multiplication and exponentiation ...

Reference is also made to the **Montgomery** multiplication **methods** as MM. .... B.sub.d ; ii the LS Carry Out bit from the **Carry Save** Accumulator; ...

[www.patentmonkey.com/PM/patentid/6748410.aspx](http://www.patentmonkey.com/PM/patentid/6748410.aspx) - 250k - Supplemental Result -

[Cached](#) - [Similar pages](#)

### [PDF] An Efficient Hardware Architecture for Factoring Integers with the ...

File Format: PDF/Adobe Acrobat - [View as HTML](#)

While in [6] a structure with **carry-save** adders and redundant ..... [9] P. **Montgomery**,

"Speeding up the Pollard and elliptic curve **methods** of factorization" ...

[cr.yp.to/bib/2005/franke-ecm.pdf](http://cr.yp.to/bib/2005/franke-ecm.pdf) - [Similar pages](#)

### [PDF] A Complexity-Effective Version of Montgomery's Algorithm

File Format: PDF/Adobe Acrobat - [View as HTML](#)

The standard **Montgomery** method for modular multiplication is ... **Carry save** adders have a latency of O(1) in comparison to standard ripple ...

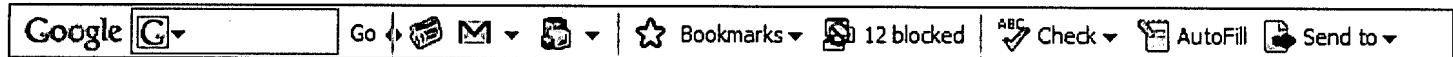
[www.ece.rochester.edu/~albonesi/wced02/papers/bunimov.pdf](http://www.ece.rochester.edu/~albonesi/wced02/papers/bunimov.pdf) - [Similar pages](#)

### Apparatus & method for modular multiplication & exponentiation ...

Apparatus as in claim 1 wherein summations into the **carry save** adder are ..... Reference is also made to the **Montgomery** multiplication **methods** as MM. ...

1 [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [Next](#)

Free! Get the Google Toolbar. [Download Now](#) - [About Toolbar](#)



---

Montgomery method carry-save pdf

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied? Help us improve](#)

---

©2007 Google - [Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

[Google](#)

bernard plessier

[Advanced Search](#)  
[Preferences](#)

Web

Results 1 - 10 of about 43,400 for bernard plessier. (0.35 seconds)Did you mean: bernard pelletier

### DBLP: Bernard Plessier

**Bernard Plessier.** List of publications from the DBLP Bibliography Server - FAQ ... 6,  
**Bernard Plessier**, Gary D. Hachtel, Fabio Somenzi: Extended BDDs: ...  
[www.informatik.uni-trier.de/~ley/db/indices/a-tree/p/Plessier:Bernard.html](http://www.informatik.uni-trier.de/~ley/db/indices/a-tree/p/Plessier:Bernard.html) - 10k -  
[Cached](#) - [Similar pages](#)

### Verification of systems containing counters

**B. Plessier**, E. Schwars, F. Somenzi, "ATPG Aspects of FSM"~erification", I(TCAD-90, pp. 134-137, November 1990. .... **Bernard F. Plessier** ...  
[portal.acm.org/citation.cfm?id=304032.304081](http://portal.acm.org/citation.cfm?id=304032.304081) - [Similar pages](#)

### Algorithms for approximate FSM traversal

**Bernard Plessier**: Hyunwoo Cho, Gary D. Hachtel, Enrico Macii, Fabio Somenzi, Fabio Somenzi: Adnan Aziz, R. Iris Bahar, Ruth Iris Bahar, Brian Bailey ...  
[portal.acm.org/citation.cfm?id=164555&dl=GUIDE&coll=GUIDE&CFID=15151515&CFTOKEN=6184618](http://portal.acm.org/citation.cfm?id=164555&dl=GUIDE&coll=GUIDE&CFID=15151515&CFTOKEN=6184618) - [Similar pages](#)  
[ More results from [portal.acm.org](http://portal.acm.org) ]

### DBLP: Fabio Somenzi

67, **Bernard Plessier**, [8] [11] [12] [16] [22] [26] [29] [42] [50]. 68, Massimo Poncino, [27] [28] [33] [39] [43] [62]. 69, Paolo Prinetto, [1] [2] ...  
[www.sigmod.org/dblp/db/indices/a-tree/s/Somenzi:Fabio.html](http://www.sigmod.org/dblp/db/indices/a-tree/s/Somenzi:Fabio.html) - 94k -  
[Cached](#) - [Similar pages](#)

### DBLP: Gary D. Hachtel

38, **Bernard Plessier**, [8] [12] [13] [20] [23] [34]. 39, Massimo Poncino, [24] [25] [29] [32] [35]. 40, Shaz Qadeer, [39] [40] ...  
[www.sigmod.org/dblp/db/indices/a-tree/h/Hachtel:Gary\\_D=.html](http://www.sigmod.org/dblp/db/indices/a-tree/h/Hachtel:Gary_D=.html) - 50k -  
[Cached](#) - [Similar pages](#)  
[ More results from [www.sigmod.org](http://www.sigmod.org) ]

### oDOBS - Author page: Fabio Somenzi

Enrico MACII, **Bernard PLESSIER**, Fabio SOMENZI: Formal verification of digital systems by automatic reduction of data paths. ...  
[lupus.cs.uni-dortmund.de:8080/odobs/author;jsessionid=132C989092F5D4BC1FFD576DF28C6F53?id=413730](http://lupus.cs.uni-dortmund.de:8080/odobs/author;jsessionid=132C989092F5D4BC1FFD576DF28C6F53?id=413730) - 95k -  
[Cached](#) - [Similar pages](#)

### Efficient BDD Algorithms for FSM Synthesis and Verification ...

Document: Details Efficient Formal Design Verification: Data Structure + Algorithms (1994)  
Rajeev K. Ranjan, Adnan Aziz, Robert K. Brayton, **Bernard Plessier** ...  
[citeseer.ist.psu.edu/article/ranjan95efficient.html](http://citeseer.ist.psu.edu/article/ranjan95efficient.html) - 5k - [Cached](#) - [Similar pages](#)

### Symmetry Detection and Dynamic Variable Ordering of Decision ...

Shipra Panda, Fabio Somenzi, **Bernard F. Plessier** ... S. Panda, F. Somenzi, and B.F. Plessier. Symmetry Detection and Dynamic Variable Ordering of Decision ...  
[citeseer.ist.psu.edu/panda96symmetry.html](http://citeseer.ist.psu.edu/panda96symmetry.html) - 27k - [Cached](#) - [Similar pages](#)  
[ More results from [citeseer.ist.psu.edu](http://citeseer.ist.psu.edu) ]

### [PDF] OCRed document

File Format: PDF/Adobe Acrobat  
including **Bernard Plessier**, Carl Pixley from (Motor- ola SSDT), Rajeev Ranjan (U.C.

Berkeley), and. Hoang Quan, Nigel Allison and Maria Hathaway ...  
ieeexplore.ieee.org/iel2/3317/9950/00472465.pdf?arnumber=472465 - [Similar pages](#)

[PDF] [ICCD'97: Intertwined development and formal verification of a 60 ...](#)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

begun by **Bernard Plessier** and completed by Matt Kauf- man over a period of about three months, starting with. English documentation of a 60x bus protocol ...  
[www.iccd-conference.org/proceedings/1997/82060025.pdf](http://www.iccd-conference.org/proceedings/1997/82060025.pdf) - [Similar pages](#)

Did you mean to search for: [bernard pelletier](#)

[1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [Next](#)

Download [Google Pack](#): free essential software for your PC

---

bernard plessier

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied? Help us improve](#)

---

©2007 Google - [Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

**Google**

bernard plessier

[Advanced Search](#)[Preferences](#)**Web**Results 11 - 20 of about 43,400 for **bernard plessier**. (0.08 seconds)**[PDF] Intertwined Development and Formal Verification of a 60x Bus Model ...**

File Format: PDF/Adobe Acrobat

begun by **Bernard Plessier** and completed by Matt Kaufmann over a period of about three ... **Bernard Plessier** wrote the first model and specifications. ...ieeexplore.ieee.org/iel3/4973/13677/00628845.pdf?arnumber=628845 - [Similar pages](#)**Acknowledgments**... In-Ho Moon, Curt Musfeldt, Shipra Panda, Abelardo Pardo, **Bernard Plessier**, Kavita Ravi, Hyongkyoon Shin, Alan Shuler, Arun Sivakumaran, Jorgen Sivesind. ...vlsi.colorado.edu/~fabio/CUDD/node6.html - 5k - [Cached](#) - [Similar pages](#)**Shipra's Work Page Test**Shipra Panda, Fabio Somenzi, and **Bernard Plessier**, "Symmetry Detection and Dynamic Variable Ordering of Decision Diagrams," ICCAD-94: ACM/IEEE International ...www.ece.cmu.edu/~spanda/work.html - 2k - [Cached](#) - [Similar pages](#)**[PDF] Computer Aided Design and Test**File Format: PDF/Adobe Acrobat - [View as HTML](#)Carl Pixley, **Bernard Plessier**, Hyumoro Cho ..... **Bernard Plessier**. Dept. of Electrical and Computer Engineering Motorola Inc. ...www.dagstuhl.de/Reports/9507.pdf - [Similar pages](#)**International Conference on Computer Aided Design**by: Enrico Macii, **Bernard Plessier**, Fabio Somenzi. On average power dissipation and random pattern testability of CMOS combinational logic networks ...wotan.liu.edu/docis/dbl/iccadi/index.html - 360k - [Cached](#) - [Similar pages](#)**Soptol, la société**

pointrf2.gif (864 octets) SOPTOL was created on the 15th of January 1987 by Messrs

**Bernard PLESSIER** and Francis ORIER aT 59 rue de l'esplanade in HAM. ...www.soptol.com/english/societe.htm - 11k - [Cached](#) - [Similar pages](#)**Volume 3 "Computer-Aided Verification '90", Clarke & Kurshan, Eds.**... on the Interface between Formal Verification and ATPG Hyunwoo Cho, Gary Hachtel, Seh-Woong Jeong, **Bernard Plessier**, Eric Schwarz, and Fabio Somenzi 615 ...dimacs.rutgers.edu/Volumes/Vol03.html - 18k - [Cached](#) - [Similar pages](#)**Rajeev's Publications**

... of IEEE/ACM International Workshop on Logic Synthesis, Lake Tahoe, May 1995, with

Adnan Aziz, **Bernard Plessier**, Carl Pixley and R. K. Brayton ...

embedded.eecs.berkeley.edu/Alumni/rajeev/publications/publications.html - 6k -

[Cached](#) - [Similar pages](#)**Libra: CUDD: CU Decision Diagram Package Release 2.2.0**

Symmetry Detection and Dynamic Variable Ordering of Decision Diagrams(1996)

(citation:22) · Shipra Panda Fabio Somenzi **Bernard F. Plessier** ...libra.directtaps.net/paperdetail.aspx?id=246957 - 32k - [Cached](#) - [Similar pages](#)**[PS] Copyright c1997 by the Association for Computing Machinery, Inc. Permission to**File Format: Adobe PostScript - [View as Text](#)**Bernard Plessier**, the designer of FIRE, was of immense help in formalizing the specifications of the design. REFERENCES. [1] E. A. Emerson, "Temporal and ...research.microsoft.com/~qadeer/docs/dac97.fire.ps - [Similar pages](#)

bernard plessier

[Search within results](#) | [Language Tools](#) | [Search Tips](#)

---

©2007 Google - [Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)